REMARKS

Claims 1-3, 6, 13, 16, 20, 23-25, 28, and 32-33 are currently amended. Claims 4-5, 14-15, 21-22, 26, and 29 are canceled. Claims 1-3, 6-13, 16-20, 23-25, 27-28, and 30-33 are pending and are listed below. In view of the foregoing amendments and the following remarks, Applicant respectfully requests that this application be allowed and forwarded on to issuance.

§112 Rejections

In the current Action, the Office rejects claims 18, 19, and 27 under 35 U.S.C. §112 as failing to provide an antecedent basis for an element in the claims. *Office Action mailed 12/04/2006*, p. 2. Applicant respectfully submits, however, that Applicant has been previously amended these claims in order to obviate the grounds for these rejections. It therefore appears that the Office inadvertently fails to remove these rejections in the current Office Action.

Applicant therefore once more respectfully requests that the Office withdraw the rejections.

§101 Rejections

Claims 25, 27-30, and 32-33 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Applicant respectfully traverses the rejections. Nevertheless, Applicant has amended these claims for the sole purpose of advancing prosecution and without conceding the propriety of the Office's rejections.

Claim 25 has been amended to recite, in whole, the subject matter of previously-dependent claim 26. In particular, claim 25 has been amended to recite

"a storage medium configured to retain the binary information". Applicant notes that claim 26 does not stand rejected under 35 U.S.C. §101. Applicant therefore respectfully submits that this amendment obviates the grounds for the Office's rejection and respectfully requests that the rejection be withdrawn.

Claim 27 depends from claim 25 and, due to this dependency, recites statutory subject matter. Applicant therefore respectfully requests that the rejection of this claim under 35 U.S.C. §101 be withdrawn.

Claim 28 has also been amended and, as amended, now recites "a storage medium configured to retain the binary files". Applicant respectfully submits that this "storage medium" represents that the element present in previously-dependent claim 26. Furthermore and as noted immediately above, claim 26 does not stand rejected under 35 U.S.C. §101, apparently for its inclusion of this "storage medium". Applicant therefore respectfully submits that this amendment to claim 28 obviates the grounds for the Office's rejection, and respectfully requests that the rejection be withdrawn.

Claims 30 and 32 have been similarly amended to recite "a database *embodied as a computer-readable storage medium*". (emphasis added). Again, Applicant respectfully submits that such an amendment results in claims that recite statutory subject matter for the same reasons discussed above in regards to claims 25 and 28. That is, these claims now each recite an element that the Office treats as resulting in a claim directed to statutory subject matter. Applicant therefore respectfully submits that these amendments obviates the grounds for the Office's rejections, and respectfully requests that the rejections be withdrawn.

Claim 31 and 33 depend from claims 30 and 32, respectively, and, due to this dependency, recite statutory subject matter. Applicant therefore respectfully requests that the rejection of these claims under 35 U.S.C. §101 be withdrawn.

§102 Rejections

Claims 1-18 and 20-33 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 6,199,204 to Donohue (hereinafter, "Donohue"). Applicant respectfully traverses the rejections. Nevertheless, Applicant has amended some of the claims for the sole purpose of advancing prosecution, as discussed above.

Claim 1 has been amended and, as amended, recites a processor-readable medium having a tangible component and comprising processor-executable instructions configured for:

- receiving a binary signature at a server computing device;
- receiving a security patch at the server computing device;
- identifying, from the server computing device, a vulnerable binary file located on a client computing device based on the binary signature, the client computing device being remote from the server computing device; and
- updating, from the server computing device, the vulnerable binary file located on the client computing device with the security patch.

Applicant respectfully submits that the Office fails to show how Donohue discloses at least the added elements of Applicant's amended claim 1. For instance, Applicant respectfully submits that the Office fails to show how Donohue discloses "receiving a binary signature [and]...a security patch *at [a] server computing device*", "identifying, *from the server computing device*, a

vulnerable binary file *located on a client computing device*", and "updating, *from the server computing device,* the vulnerable file *located on the client computing device*", as recited in Applicant's claim. (emphasis added). Furthermore, Applicant notes that during the above-referenced interview, the Examiner appeared to agree that Donohue discloses no such claim elements.

For at least these reasons, this claim stands allowable.

Claims 2-4 and 7 depend from claim 1 and, as such, the remarks made above in regards to claim 1 apply equally to these claims. The rejections of these claims are also improper as failing to disclose these claims' own recited features which, in combination with those recited in claim 1, are not shown to be disclosed in the reference of record, either singly or in combination with one another.

Claim 8 recites a processor-readable medium having a tangible component and comprising processor-executable instructions configured for (emphasis added):

- receiving a binary signature that identifies a security vulnerability in a binary file;
- receiving a security patch configured to fix the security vulnerability in the binary file; and
- ***distributing the binary signature and the security patch to a plurality of servers.***

Donohue, meanwhile, describes an updater agent that is associated with a computer program and that accesses relevant network locations to download and install updates to the agent's associated program. The agent, which resides on a conventional computer, downloads and installs the updates onto the computer if those updates satisfy predefined update criteria of the updater agent. *Donohue*, abstract. The predefined criteria may include the time period between searches for

updates and whether the computer user has selected to receive all updates or only certain ones. In a preferred embodiment, the updater agent searches the internet via a search engine to find the network location where an update list is kept. Donohue's updater agent then compares available software updates with installed software on the computer to determine which updates are relevant. The updater agent then compares these updates with the predefined criteria to determine whether or not to download the updates. *Id.* at column 4, line 14 through column 5, line 10.

In making out a rejection of Applicant's claim 1, the Office contends that Donohue anticipates. Applicant respectfully disagrees, and instead submits that the Office fails to show how Donohue discloses "distributing [a] binary signature and [a] security patch to a plurality of servers", as recited in Applicant's claim. In stating that Donohue discloses this element, the Office appears to chiefly rely on Donohue's column seven, lines 55-65. Applicant reproduces this passage for the Office's convenience:

> The system 10 of FIG. 1 is shown connected within a network 100 of computers including a number of remote server systems (50,50') from which software resources are available for applying updates to programs installed on the local system 10. *Each server system includes within storage a list 60 of the latest versions of, and patches for, **software products which are available from that server**. Each vendor is assumed here to make available via their Web sites such a list 60 of software updates* (an example of which is shown in FIG. 2) comprising their product release history, in a format which is readable by updater components...
>
> *Donohue*, col. 7, lines 55-65 (emphasis added).

Applicant submits that the above passage merely discusses a network 100 that includes multiple remote server systems, with each server containing a list 60

of the latest versions, and patches for, software products available from that particular server. In other words, this passage merely states that each server within the network contains updates and patches for whatever software product the server is associated with. Donohue's updater agent may then access the relevant server and download the server's list of updates.

First, Applicant respectfully submits that this passage fails to disclose "distributing [a] binary signature and [a] security patch to a plurality of servers". Instead, this passage merely states that each server in the network *contains* a list of updates. Furthermore, the updater agent on a computer goes out and obtains this list—but Donohue does not disclose distributing that list to a plurality of other servers.

Furthermore, Applicant submits that each server within the Donohue network 100 appears to correspond to different software products. Each server thus contains a list of updates and patches for a particular software product. As such, each server contains *different* updates and patches. Therefore, even assuming that "each vendor" distributes these updates and patches to a corresponding server, not a single vendor has been shown to distribute these updates and patches to a "plurality of servers". The cited portion of Donohue therefore fails to disclose "distributing ***the*** binary signature and ***the*** security patch *to a plurality of servers*", as recited in Applicant's claim. (emphasis added). Applicant further notes that this claim does not merely recite distributing *any sort of* binary signature and security patch, but rather recites distributing *the* received binary signature and *the* received security patch to a plurality of servers—and not to a single corresponding server.

For at least this reason, this claim stands allowable.

Claims 9 and 10 depend from claim 8 and, as such, the remarks made above in regards to claim 8 apply equally to these claims. The rejections of these claims are also improper as failing to disclose these claims' own recited features which, in combination with those recited in claim 8, are not shown to be disclosed in the reference of record, either singly or in combination with one another.

Claim 11 recites a processor-readable medium having a tangible component and comprising processor-executable instructions configured for (emphasis added):

- receiving a binary signature from a server;
- searching for the binary signature in binary files located on a client computer;
- ***sending a request from the client computer to the server for a security patch if a binary file is found that includes the binary signature***;
- receiving the security patch from the server; and
- updating on the client computer the binary file with the security patch..

In making out a rejection of this claim, the Office states that Donohue anticipates all of the elements of the claim. Applicant respectfully disagrees, and submits that the Office at least fails to show how Donohue discloses "*sending a request from the client computer to the server for a security patch if a binary file is found that includes the binary signature*", as recited in Applicant's claim. (emphasis added). In this regard, Applicant submits that: (1) the cited portion of Donohue fails to disclose this claim element, and (2) Donohue as a whole fails to disclose this element.

First, Applicant submits that the cited portion of Donohue fails to disclose this claim element. In stating that Donohue does indeed anticipate this element,

the Office cites to Donohue's column 13, lines 6-10. Applicant reproduces this passage, as well as some surrounding text, for the Office's convenience:

> ***Structure of Updater Component***
>
> The structure of an updater component comprises data, methods for operating on that data, and a public application programming interface (API) which allows other updater components to contact and communicate with it. ***This structure will now be described in detail.***
>
> * * *
>
> ***Receive_Event(event details)***
>
> ***When an updater component receives a request to update, it must inform the calling updater component when it has completed the update or otherwise*** e.g. if it failed for some reason. The updater component performing the update on behalf of another updater component will call this function of the requesting updater component to communicate success of the update or otherwise.
>
> *Donohue*, col. 11, lines 20-25, col. 13, lines 5-13 (emphasis added).

As the first of the two passages explains, the second and cited Donohue passage relates to the *structure of the updater component that resides on a conventional computer*. With this context in mind, the cited passage then explains that a first "updater component [may] receive[] a request to update" from another "calling updater agent". As discussed in portions of Donohue following this passage, the cited passage relates to multiple updater components for differing associated computer programs communicating with one another. As Donohue describes, an updater component associated with a first software program may recognize that another second software program is a pre-requisite to updating the first software program. This first updater component may then "call" an updater

component associated with the second computer program and request that the latter updater component update the second computer program. *Id.* at col. 13, lines 22-54. Applicant submits that cited passage of Donohue merely relates to this interrelationship between multiple updater components residing on a same conventional computer.

Applicant respectfully submits that this passage—relating to requests *between* updater components, all resident on a single computer—fails to disclose "*sending a request* ***from the client computer to the server*** *for a security patch if a binary file is found that includes the binary signature*", as recited in Applicant's claim. (emphasis added). In fact, Applicant respectfully submits that this cited passage fails to relate to the sending of a request to any sort of server whatsoever. Additionally, the described communication between updater components fails to disclose "request[ing]…a security patch", as well as sending a request "if a binary file is found that includes the binary signature". Applicant thus respectfully submits that the Office fails to show how Donohue anticipates Applicant's claim.

For at least this reason, this claim stands allowable.

Secondly, Applicant respectfully submits that Donohue as a whole at least fails to disclose "*sending a request from the client computer to the server for a security patch* ***if a binary file is found that includes the binary signature***", as recited in Applicant's claim. (emphasis added).

As discussed above, Donohue has at most been shown to disclose an updater agent that is associated with a computer program and that *accesses relevant network locations and automatically downloads and installs any available updates to its associated program. Donohue*, abstract (emphasis added).

As such, Donohue's updater agent merely retrieves available updates from a network location and automatically installs them on a computer.

Applicant contrasts this Applicant's claim 11, which recites "receiving a binary signature from a server; *searching for the binary signature* in binary files located on a client computer; [and] *sending a request from the client computer to the server for a security patch* ***if a binary file is found that includes the binary signature***". (emphasis added). Donohue's updater agent does not so "receiv[e]…, search[], [and] request[]"—the updater agent merely retrieves the updates and installs them.

For at least this additional reason, this claim stands allowable.

Claim 12 depends from claim 11 and, as such, the remarks made above in regards to claim 11 apply equally to this claim. The rejection of this claim is also improper as failing to disclose this claim's own recited features which, in combination with those recited in claim 11, are not shown to be disclosed in the reference of record, either singly or in combination with one another.

Claim 13 recites a method comprising (emphasis added):

- receiving a binary signature from a server and at a client computer;
- searching on the client computer for a vulnerable file based on the binary signature;
- ***if a vulnerable file is found on the client computer, requesting a security patch from the server***;
- receiving the security patch from the server and at the client computer in response to the request for the security patch from the client computer; and
- fixing the vulnerable file with the security patch received from the server.

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 11. Thus, for at least the reasons discussed above in regards to claim 11, Applicant respectfully submits that the Office fails to show how Donohue anticipates this claim and, further, that Donohue as a whole fails to so anticipate. Namely, Donohue fails to disclose "if a vulnerable file is found on the client computer, requesting a security patch from the server", as recited in Applicant's claim. Instead, Donohue at most has been shown to describe retrieving and automatically installing updates to a computer.

For at least this reason, this claim stands allowable.

Claims 16-18 depend from claim 13 and, as such, the remarks made above in regards to claim 13 apply equally to these claims. The rejections of these claims are also improper as failing to disclose these claims' own recited features which, in combination with those recited in claim 13, are not shown to be disclosed in the reference of record, either singly or in combination with one another.

Claim 20 recites method comprising:

- receiving, at a scan/patch server, a binary signature and a security patch from a distribution server;
- searching, by the scan/patch server, on a client computer for a vulnerable file associated with the binary signature; and
- if a vulnerable file is found, fixing, by the scan/patch server, the vulnerable file on the client computer with the security patch.

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim

1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that Donohue does not anticipate this claim. For instance, Applicant respectfully submits that the Office fails to show how Donohue discloses "receiving, *at a scan/patch server*, a binary signature and a security patch", "searching, *by the scan/patch server, on a client computer* for a vulnerable file associated with the binary signature", and "fixing, *by the scan/patch server*, the vulnerable file *on the client computer*", as recited in Applicant's claim. (emphasis added). Furthermore, Applicant notes that during the above-referenced interview, the Examiner appeared to agree that Donohue discloses no such claim elements.

For at least these reasons, this claim stands allowable.

Claim 23 recites a computer comprising (emphasis added):

- means for receiving, at a client computer, a binary signature from a server;
- means for searching for a vulnerable file located on the client computer based on the binary signature;
- ***means for requesting, by the client computer, a security patch from the server if a vulnerable file is found on the client computer***;
- means for receiving the security patch from the server at the client computer responsive to the request for the security patch; and
- means for fixing the vulnerable file with the security patch received from the server.

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 11. Thus, for at least the reasons discussed above in regards to claim 11, Applicant respectfully submits that the Office fails to show how Donohue

anticipates this claim and, further, that Donohue as a whole fails to so anticipate. Namely, Donohue fails to disclose "means for requesting, by the client computer, a security patch from the server if a vulnerable file is found on the client computer", as recited in Applicant's claim. Instead, Donohue at most has been shown to describe retrieving and automatically installing updates to a computer.

For at least this reason, this claim stands allowable.

Claim 24 recites a server comprising:

- means for receiving, at a scan/patch server, a binary signature and a security patch from a distribution server;
- means for scanning, from the scan/patch server, a client computer for a vulnerable file associated with the binary signature; and
- means for fixing, from the scan/patch server, the vulnerable file on the client computer with the security patch if a vulnerable file is found on the client computer.

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that Donohue does not anticipate this claim. For instance, Applicant respectfully submits that the Office fails to show how Donohue discloses "means for receiving, *at a scan/patch server*, a binary signature and a security patch", "means for scanning, *from the scan/patch server, a client computer* for a vulnerable file associated with the binary signature", and "means for fixing, *from the scan/patch server*, the vulnerable file *on the client computer*", as recited in Applicant's claim. (emphasis added). Furthermore, Applicant notes that during the above-referenced interview, the Examiner appeared to agree that Donohue discloses no such claim elements.

For at least these reasons, this claim stands allowable.

Claim 25 recites a computer having a tangible component and comprising (emphasis added):

- binary information;
- a storage medium configured to retain the binary information;
- a scan module configured to receive a binary signature from a server and scan the binary information on the computer for the binary signature; and
- ***a patch module configured to request a security patch from a server and install the security patch from the server if the binary signature is found in the binary information on the computer.***

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 11. Thus, for at least the reasons discussed above in regards to claim 11, Applicant respectfully submits that the Office fails to show how Donohue anticipates this claim and, further, that Donohue as a whole fails to so anticipate. Namely, Donohue fails to disclose "a patch module configured to request a security patch from a server and install the security patch from the server if the binary signature is found in the binary information on the computer", as recited in Applicant's claim. Instead, Donohue at most has been shown to describe retrieving and automatically installing updates to a computer.

For at least this reason, this claim stands allowable.

Claim 27 depends from claim 25 and, as such, the remarks made above in regards to claim 25 apply equally to this claim. The rejection of this claim is also improper as failing to disclose this claim's own recited features which, in

combination with those recited in claim 25, are not shown to be disclosed in the reference of record, either singly or in combination with one another.

Claim 28 recites a computer having a tangible component and comprising (emphasis added):

- binary files;
- a storage medium configured to retain the binary files;
- a binary signature; and
- a security patch module configured to receive the binary signature from a server and to scan the binary files on the computer in search of the binary signature;
- a binary file that includes the binary signature; and
- a security patch;
- ***wherein the security patch module is further configured to request the security patch from the server upon locating the binary signature within the binary file***, and to apply the security patch to the binary file that includes the binary signature.

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 11. Thus, for at least the reasons discussed above in regards to claim 11, Applicant respectfully submits that the Office fails to show how Donohue anticipates this claim and, further, that Donohue as a whole fails to so anticipate. Namely, Donohue fails to disclose a "security patch module [that] is [] configured to request the security patch from the server upon locating the binary signature within the binary file", as recited in Applicant's claim. Instead, Donohue at most has been shown to describe retrieving and automatically installing updates to a computer.

For at least this reason, this claim stands allowable.

Claim 30 recites a distribution server having a tangible component and comprising (emphasis added):

- a database embodied as a computer-readable storage medium; and
- ***a distribution module configured to*** receive a binary signature and a security patch, store the binary signature and the security patch in the database, and ***distribute the binary signature and the security patch to a plurality of servers***.

In making out a rejection of this claim, the Office states that Donohue anticipates all of the elements of the claim. Applicant respectfully submits, however, that the Office fails to show how Donohue anticipates for at least the reasons discussed above in regards to claim 8. Namely, Donohue fails to disclose "a distribution module configured to...distribute the binary signature and the security patch *to a plurality of servers*", as recited in Applicant's claim. (emphasis added).

For at least this reason, this claim stands allowable.

Claim 31 depends from claim 30 and, as such, the remarks made above in regards to claim 30 apply equally to this claim. The rejection of this claim is also improper as failing to disclose this claim's own recited features which, in combination with those recited in claim 30, are not shown to be disclosed in the reference of record, either singly or in combination with one another.

Claim 32 recites a server having a tangible component and comprising:

- a binary signature associated with a security vulnerability in a binary file;
- a security patch configured to fix the security vulnerability in the binary file;
- a database embodied as a storage medium and configured to store the binary signature and the security patch;
- a scan module configured to scan, from the server, binary files on a client computer for the binary signature and to

update, from the server, the binary file on the client computer with the security patch if the binary signature is found, wherein the client computer is remote from the server.

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that Donohue does not anticipate this claim. For instance, Applicant respectfully submits that the Office fails to show how Donohue discloses "a scan module configured to scan, *from the server*, binary files *on a client computer* for the binary signature and to update, *from the server*, the binary file *on the client computer* with the security patch if the binary signature is found, *wherein the client computer is remote from the server*", as recited in Applicant's claim. (emphasis added). Furthermore, Applicant notes that during the above-referenced interview, the Examiner appeared to agree that Donohue discloses no such claim elements.

For at least this reason, this claim stands allowable.

Claim 33 depends from claim 32 and, as such, the remarks made above in regards to claim 32 apply equally to this claim. The rejection of this claim is also improper as failing to disclose this claim's own recited features which, in combination with those recited in claim 32, are not shown to be disclosed in the reference of record, either singly or in combination with one another.

§103 Rejections

Claim 19 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Donohue in view of U.S. Patent No. 5,930,504 to Gabel (hereinafter, "Gabel"). Applicant respectfully traverses this rejection.

Claim 19 ultimately depends from independent claim 13. As discussed above, Applicant submits that claim 13 stands allowable. Applicant submits that Donohue not only fails to disclose elements of claim 13, but also fails to teach or suggest such elements. Furthermore, in the rejection of claim 19 Gabel has not been cited to teach or suggest claims elements that the rejection of base claim 13 lacks. Thus, claim 19 stands allowable as depending from an allowable base claim. The rejection of this claim is also improper as failing to disclose this claim's own recited features which, in combination with those recited in claim 13, are not shown to be taught or suggested in the reference of record, either singly or in combination with one another.

Conclusion

All of the claims are in condition for allowance. Accordingly, Applicant requests a Notice of Allowability be issued forthwith. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant respectfully requests a telephone call for the purpose of scheduling an interview.

Respectfully submitted,

Dated: 2007/03/05

By: 

Robert G. Hartman
Reg. No. 58,970
(509) 324-9256 ext 265